

UNITED STATES DISTRICT COURT

for the  
Eastern District of Wisconsin

In the Matter of the Search of:

the premises of iSupply West + Vape – Electronic Repairs  
and Sales, located at 1315 West Mason Street, Unit 1, Green  
Bay, Wisconsin 54303, more fully described in Attachment  
A3.

Case No. 19-MJ-1285

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

See Attachment A3.

located in the Eastern District of Wisconsin, there is now concealed:

See Attachment B3.

The basis for the search under Fed. R. Crim P. 41(c) is:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of: 18 U.S.C. § 922(a)(1)(A), § 922(d), § 922(a)(6), § 924(b), § 922(a)(9), § 924(h), § 924(g), § 371 and 22 U.S.C. § 2778(b)(2)(c)

The application is based on these facts: See attached affidavit.

☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



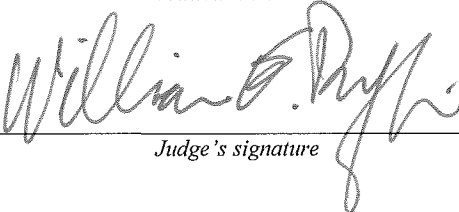
Applicant's signature

Special Agent Ryan Arnold, ATF

Printed Name and Title

Sworn to before me and signed in my presence:

Date: 9/9/19



Judge's signature

City and State: Milwaukee, Wisconsin

Honorable William E. Duffin

U.S. Magistrate Judge

**AFFIDAVIT IN SUPPORT OF  
APPLICATIONS FOR SEARCH WARRANTS**

I, Ryan Arnold, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of applications under Rule 41 of the Federal Rules of Criminal Procedure for warrants to search the following premises (collectively, “PREMISES”) and the person of JOE ROBLES (DOB: 11/10/1986), further described in Attachments A1, A2, A3, and A4, for the things described in Attachments B1, B2, B3, and B4:

- A1. The premises located at **915 North Locust Street, Green Bay, Wisconsin 54303**, more fully described as a single story, single family brick residence with a grey roof. That premises has an attached single garage painted white to the south of the front door and a chain link fence on the north side of the residence.
- A2. The premises located at **2100 Memorial Drive, Apartment 204, Green Bay, Wisconsin 54303**, more fully described as a two-bedroom apartment located in the Northern Pines Apartment Complex. The apartment complex is a two story structure with cream and white colored siding and a grey roof. Unit 204 is located on the second story of the building with the numerals “204” prominently displayed on the front door to the apartment.
- A3. The premises of **iSupply West + Vape – Electronic Repairs and Sales**, more fully described as a business located at 1315 West Mason Street, Unit 1, Green Bay, Wisconsin 54303. This business is located in the Ridgeview Center, which contains

approximately four separate businesses. The building is white and stone in color with black support beams and a brown roof. The numerals "1315" are prominently displayed on the sign directly in front of the building. The business bears a white sign with the words "I supply vape" located directly above the front door entrance.

**A4. The person of Joe Robles (DOB: 11/10/1986).**

2. I am a Special Agent with the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) and have been since April 2015. With the ATF, I have participated in numerous investigations into firearms trafficking, unlawful possession of firearms by prohibited persons, unlawful use of firearms, drug trafficking, and arson. I have previously investigated firearms trafficking organizations that purchase, transport, and traffic firearms both nationally and internationally.

3. Before that, I was a Special Agent with the United States Secret Service for nearly five years. My duties included providing and planning dignitary protection, drafting and executing federal search warrants, and conducting investigations into organized crime networks, threats against Secret Service protectees, fraud networks, counterfeit currency, and other financial crime investigations.

4. Before I joined the Secret Service, I served as a police officer with the Chicago Police Department (CPD) in Illinois. During part of my career as a police officer, I was assigned to the Gang Enforcement Unit of the Organized Crime Division, where I conducted investigations

into street gangs, narcotics distribution, firearms violations, robbery, and home invasions.

5. I obtained a Master of Arts from American Military University with a degree in National Security Studies and a focus on terrorism. During my studies, I successfully completed the “Drug Cartels and the Narcotics Threat” course. This course covered the organization, production, and distribution networks of drug cartels.

6. I have participated in numerous firearm trafficking and drug trafficking investigations involving the seizure of computers, cellular phones, cameras, and other digital storage devices, and the subsequent analysis of electronic data stored within these devices. On numerous occasions, this electronic evidence has proof of the crimes being investigated and corroborated information already known or suspected by law enforcement. I have regularly used electronic evidence to find proof relating to the commission of criminal offenses, including intent, motive, manner, means, and the identity of co-conspirators.

7. Based on my training, experience and participation in drug trafficking and firearms trafficking investigations, I know and have observed the following:

- a. I have relied informants to investigate firearms trafficking and drug trafficking. Through informant interviews and debriefings of individuals involved in those offenses, I have learned about the manner in which individuals and organizations finance, purchase, transport, and distribute firearms and narcotics both within and outside of Wisconsin. I have utilized informants to conduct “controlled purchases” of firearms and controlled substances from individuals, as opposed to licensed gun

dealers. I have also conducted surveillance of individuals engaged in firearms and drug trafficking and participated in the execution of numerous search warrants resulting in the seizure of drugs, firearms, ammunition, and magazines.

- b. Based on my training and experience, I have become familiar with the language utilized over the telephone to discuss firearms and drug trafficking and know that the language is often limited, guarded, and coded. I also know that firearms and drug traffickers often use electronic devices (such as computers and cellular phones) and social media to facilitate these crimes. Based on my experience, I know that firearms traffickers may keep photographs of these items on electronic devices.
- c. I also know that drug traffickers and firearms traffickers commonly possess—on their person, at their residences, at their places of business, in their vehicles, and other locations where they exercise dominion and control—firearms, ammunition, and records or receipts pertaining to such.
- d. I know that firearms traffickers and drug traffickers often put their telephones in nominee names to distance themselves from telephones that are utilized to facilitate these and related offenses. I also know that firearm and drug traffickers often use proceeds to purchase assets such as vehicles, property, jewelry, and narcotics. I also know that firearm and drug traffickers often use nominees to purchase or title these assets to avoid scrutiny from law enforcement.

8. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other investigators and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrants and does not set forth all of my knowledge about this matter.

9. There is probable cause to believe that evidence of violations of the following laws of the United States, including the things described in Attachments B1, B2, B3, and B4, will be found in the property listed in Attachments A1, A2, A3, and A4, respectively: 18 U.S.C. § 922(a)(1)(A) (engaging in a firearms business without a license), 18 U.S.C. § 922(d) (transferring a firearm to a prohibited person), 18 U.S.C. § 922(a)(6) (false statement to a federal firearms licensee), 18 U.S.C. § 924(b) (interstate or foreign transport of a firearm for a felony purpose), 18 U.S.C. § 922(a)(9) (unlawful receipt of firearms), 18 U.S.C. § 924(h) (transfer of firearm to be used in drug trafficking crime or crime of violence), 18 U.S.C. § 924(g) (interstate travel and transfer with intent to commit drug trafficking crime or crime of violence), 22 U.S.C. § 2778(b)(2)(c) (illegal export of munitions), and 18 U.S.C. § 371 (conspiracy).

#### **PROBABLE CAUSE**

10. Mexican law enforcement agents have been conducting an investigation into the Cartel Jalisco Nueva Generation (CJNG), a transnational criminal organization and drug cartel based in Mexico. Based on information shared between federal law enforcement agencies, it is known that this cartel participates in drug trafficking, firearms trafficking, and extreme acts of violence.

11. Law enforcement agencies in the United States have assisted with that investigation, when there is evidence of firearms trafficking originating in the United States. When Mexican law enforcement agencies have recovered firearms in this investigation, ATF agents in Mexico City have traced the origins of those firearms. Those traces have revealed that multiple firearms recovered from or associated with CJNG have been associated with Roland A. MUNOZ (H/M, DOB: 1980), who lives in Las Vegas, Nevada.

12. Those traces also reveal that MUNOZ's purchased firearms had a relatively short "time-to-crime." "Time-to-crime" is a common term used to describe the time between last known legal possession of a firearm (often the date of purchase from a federal firearms licensee) and the date of its first known use in a crime, often the recovery date. I know based on information published by the ATF's Violent Crime Analysis Branch (as of June 16, 2016) that the national average time for a gun to be recovered in a crime by law enforcement after the original purchase date is 10.48 years. I also know that the average time-to-crime for firearms in Wisconsin is 8.18 years.

13. A short time-to-crime is a strong indication of firearms trafficking or "straw buying," a term used to describe the purchase of a firearm for another person by false representation. Based on my training and experience, I know that "straw buying" is often used to provide a firearm to a person who cannot legally purchase one or to conceal the true owner of that firearm.

14. Seven of the firearms purchased by MUNOZ were recovered in Mexico between

August 1, 2018 and April 26, 2019 with a time-to-crime ranging from 186 days to 610 days. Several of these firearms were recovered from those associated or affiliated with CJNG. The number of recovered firearms, the relatively short time-to-crimes, and the recovery location are strongly indicative of straw purchasing and firearms trafficking.

15. MUNOZ did not report any of these firearms stolen. As described below, these firearms are expensive, and the failure to report the loss of those firearms indicates an attempt to remain undetected by law enforcement and evade documentation in reports.

16. Based on this information and the following evidence, the ATF believes that Roland MUNOZ and his associates are involved in criminal firearms trafficking.

#### **ROLAND MUNOZ**

17. In November 2018, ATF agents in Las Vegas contacted multiple federal firearms licensees (FFL) to look for firearm purchases completed by MUNOZ. In response, several FFLs provided documentation that MUNOZ purchased approximately thirty-nine (39) firearms between 2017 and 2018. I reviewed the records of MUNOZ's confirmed firearm purchases, and I noticed MUNOZ purchased multiple M240 and M249 style rifles, AK-47 style rifles, and .50 caliber rifles. I know from my training and experience that Mexican drug cartels including CJNG actively seek these firearms for their organizations.

18. On September 19, 2018, ATF agents in Mexico City traced firearms recovered after a shootout on the border states of Jalisco and Guanajuato between the Mexican law enforcement and military officers and members of the CJNG. During this incident, members of



the drug cartel were wounded and arrested, and Mexican officials seized multiple firearms and contacted the ATF to assist with firearms traces. One of the firearms recovered was traced to Roland MUNOZ with a 460 day time-to-crime (ATF Trace Number T20180287168), more fully described as follows:

- Firearm: Ohio Ordnance Works M240-SLR, a 7.62 caliber rifle, bearing serial number 240282;
- FFL: Spartan Arms, located at 8350 North Decatur Boulevard, Las Vegas, Nevada
- Purchase date: 05/12/2017
- Recovery date: 08/15/2018

19. On November 29, 2018, ATF agents in Mexico City reviewed eight firearms seized by the Mexican Federal Police in Guadalajara, Jalisco, Mexico on July 31, 2018, as part of an investigation of weapons possessed by members of CJNG. Three of the eight firearms were purchased by MUNOZ. Open source information revealed that some of the individuals associated with this investigation are believed to be the bodyguards for Ruben Oseguera Cervantes, a.k.a. El Mencho, the leader of CJNG. These individuals were armed with the following firearms purchased by MUNOZ:

- **Trace Number: T20180263717**
  - Time-to-crime: 454 days
  - Firearm: Century Arms International, Model RAS47, a 7.62 caliber

rifle, bearing serial number RAS47066876

- FFL: Bargain Pawn Inc., 1901-A Las Vegas Boulevard North, Las Vegas, Nevada
- Purchase date: 05/04/2017
- Recovery date: 07/31/2018

- **Trace Number: T20180263045**

- Time-to-crime: 205 days
- Firearm: FNH USA, LLC, Model M249S, a 5.56 caliber rifle, bearing serial number M249SA05216
- FFL: Fallout Firearm, 4310 Losee Road, Suite 9, North Las Vegas, Nevada
- Purchase date: 01/08/2018
- Recovery date: 07/31/2018

- **Trace Number: T20180263704**

- Time-to-crime: the federal firearms licensee is defunct, so the purchase date is unknown
- Firearm: U.S. Ordnance Inc., Model M60, a .308 caliber rifle, bearing serial number M60035
- FFL: U.S. Ordnance Inc., 300 West Sydney Drive, Unit 101, McCarran, Nevada

- Purchase date: unknown
- Recovery date: 07/31/2018

20. On August 14, 2019, agents queried ATF's Electronic Tracing System (eTrace) to look for additional firearms purchased by MUNOZ which were later recovered in Mexico.

Agents identified the following firearms purchased by MUNOZ and recovered by law enforcement in Mexico:

- **Trace Number: T20180289682**
  - Time-to-crime: 468 days
  - Firearm: Zastava, Model N-PAP M70, a 7.62 caliber rifle, bearing serial number N-PAP057333
  - FFL: Spartan Arms, 8350 North Decatur Boulevard, Las Vegas, Nevada
  - Purchase date: 05/04/2017
  - Recovery date: 08/15/2018
  - Recovery location: San Julian, Jalisco, Mexico, an area associated with CJNG
- **Trace Number: T20180418861**
  - Time-to-crime: 186 days
  - Firearm: Colt Model M4 Carbine, a 5.56 caliber rifle, bearing serial number CR206137

- FFL: Bass Pro Shop Outdoor World, Store 025, 8200 Dean Martin Drive, Las Vegas, Nevada
- Purchase date: 04/27/2018
- Recovery Date: 10/30/2018
- Recovery location: Juarez, Chihuahua, Mexico
- **Trace Number: T20190044885**
  - Time-to-crime: 203 days
  - Firearm: Romarm/Cugir, Model WASR-10, a 7.62 caliber rifle, bearing serial number A1-59888-18
  - FFL: The Peacemaker Firearms, 5355 South Decatur Boulevard, Suite 200, Las Vegas, Nevada
  - Purchase date: 05/19/2018
  - Recovery date: 12/08/2018
  - Recovery location: Salamanca, Guanajuato, Mexico
- **Trace Number: T20190177152**
  - Time-to-crime: 610 days
  - Firearm: Century Arms International, a 7.62 caliber rifle, bearing serial number C308E17904
  - FFL: 2<sup>nd</sup> Amendment Gun Shop, 4570 North Rancho Drive, Suite 4, Las Vegas, Nevada

- Purchase date: 08/24/2017
- Recovery date: 04/26/2019
- Recovery location: Morelia, Michoacán, Mexico

21. Based on that information, agents believed that MUNOZ was engaged in firearms trafficking across the border between the United States and Mexico. ATF agents in Las Vegas canvassed local FFLs and conducted interviews. Several times, agents were told that MUNOZ was with other individuals when purchasing firearms. Those individuals also purchased firearms similar in price, caliber, and style. One of the individuals who purchased firearms with Munoz was identified as Rudy ROBLES (W/M, DOB: 1977).

#### **RUDY ROBLES**

22. On November 7, 2018, ATF agents in Las Vegas interviewed the store manager and owner of Spartan Arms, a federal firearms licensee located at 8350 North Decatur Boulevard, Las Vegas, Nevada. Records revealed that MUNOZ purchased 14 firearms from Spartan Arms between April 15, 2017 and March 19, 2018. The FFL's store personnel identified "Rudy ROBLES" by name as a person who was with MUNOZ during a firearm purchase, based upon the Nevada drive license provided by ROBLES during a firearm purchase. Store personnel indicated that they believed that Rudy ROBLES had a business or family relationship with MUNOZ. ROBLES purchased the following firearms in and around Las Vegas in 2017:

- **Firearm: Ohio Ordnance Works, Model M2, a .308 caliber rifle, bearing serial number 12977102**

- FFL: 2<sup>nd</sup> Amendment Gun Shop, 4570 North Rancho Drive, Suite 4, Las Vegas, Nevada
- Purchase date: 05/25/2017
- **Firearm: Ohio Ordnance Works, Model M2, a 50 BMG caliber rifle, bearing serial number M2SA5016**
  - FFL: Spartan Arms, 8350 North Decatur Boulevard, Las Vegas, Nevada
  - Purchase date: 10/13/2017

23. MUNOZ was present for Rudy ROBLES's firearm purchase on October 13, 2017.

24. The firearms purchased by Rudy ROBLES are consistent with the type and caliber of firearms purchased by MUNOZ.

25. In an interview with ATF on April 15, 2019, Rudy ROBLES identified himself as MUNOZ's brother-in-law. Suspecting that Rudy ROBLES straw purchased those two firearms on behalf of MUNOZ, agents began searching for similar firearms within the ROBLES/MUNOZ family. On or about June 16, 2019, I was contacted by Nightfall Armory, a federal firearms licensee located in Phoenix, Arizona about a suspicious purchase conducted by Joe ROBLES (W/M, DOB: 11/10/1986) of Green Bay, Wisconsin.

**JOE ROBLES**

26. On June 16, 2019, Kyle Taylor of Nightfall Armory contacted agents about a suspicious purchase conducted by Joe ROBLES via Gunbroker.com. That day, Joe ROBLES purchased an Ohio Ordnance Works, Model M240 SLR, a .308 caliber rifle, bearing serial number 240319. Joe ROBLES sent Nightfall Armory a cashier's check in the amount of \$13,634 for the firearm. Mr. Taylor stated that he contacted ATF because of similarities in the type of firearm and last name of an individual previously flagged in their system—Rudy ROBLES. Nightfall Armory shipped the firearm to Nelson Tactical, a federal firearms licensee located at 1317 Velp Avenue, Green Bay, Wisconsin.

27. Nelson Tactical transferred the firearm to Joe ROBLES on June 21, 2019. On ATF Form 4473, Joe ROBLES checked the box indicating “yes” in response to question 11.a , which states as follows: “Are you the actual transferee/buyer of the firearm(s) listed on this form?”

28. I obtained and reviewed documents subpoenaed by the Grand Jury for telephone toll records, bank records, and Gunbroker.com information associated with Joe ROBLES. The information provided by Gunbroker.com revealed that Joe ROBLES purchased the following firearms from out-of-state federal firearms licensees which were later shipped to Nelson Tactical of Green Bay:

- **Firearm: Browning, Model M2HB, a .50 caliber belt-fed rifle, bearing serial number 2018514**

- Purchased from: James Coots of Summit Ordnance
- Purchase date: 05/08/2019
- Purchase price: \$10,500.00
- Shipped to: Nelson Tactical in Green Bay, Wisconsin
- Shipment date: 05/29/2019.
- ATF Form 4473 completion date: 05/30/2019
- Firearm transfer date: 05/30/2019
- Additional information: Joe ROBLES also purchased a Colt, Model Target, a .223 caliber rifle, bearing serial number CST001597, for \$1,285 from Nelson Tactical on that date.
- **Firearm: Ohio Ordnance Works, Model M240-SLR, a .308 caliber belt fed rifle, bearing serial number 240319**
  - Purchased from: Nightfall Armory
  - Purchase date: 06/10/2019
  - Purchase price: \$13,634.00
  - Shipped to: Nelson Tactical in Green Bay, Wisconsin
  - Shipment date: 06/19/2019
  - ATF Form 4473 completion date: 06/21/2019.
  - Firearm transfer date: 06/21/2019
- **Firearm: DS Arms, Model RPD Carbine, a 7.62x39 caliber belt-fed**



**rifle, bearing serial number TP0028**

- Purchased from: Dennis Barbini
- Purchase date: 06/28/2019
- Purchase price: \$3000.00
- Shipped to: Nelson Tactical in Green Bay, Wisconsin
- Shipment date: 06/29/2019.
- Additional information: Joe ROBLES attempted to acquire this firearm on July 12, 2019. He was denied this firearm as a result of the FBI's National Instant Criminal Background Check System (NICS). I suspect that this was in error, because the query appears to have the wrong information for Joe ROBLES. Joe ROBLES did not contact Nelson Tactical about the status of this firearm until September 5, 2019.

- **Firearm: DS Arms, Model RPDS, a 7.62x39 caliber belt-fed rifle, bearing serial number RPDS 012885**

- Purchased from: Classic Jewelry and Loan
- Purchase date: 07/03/2019
- Purchase price: \$2,729.99
- Shipped to: Nelson Tactical of Green Bay, Wisconsin
- Shipment date: 07/05/2019

- Additional information: Joe ROBLES attempted to acquire this firearm on July 12, 2019. He was denied this firearm as a result of the FBI's National Instant Criminal Background Check System (NICS). I suspect that this was in error, because the query appears to have the wrong information for Joe ROBLES. Joe ROBLES did not contact Nelson Tactical about the status of this firearm until September 5, 2019.

29. I also obtained and reviewed financial information for Joe ROBLES from Wells Fargo bank. Those statements and financial records indicate that Joe ROBLES does not have the funds to legitimately purchase \$29,863.99 in firearms within a 90 day period.

30. I also noted that ROBLES paid for the M240 purchase using a cashier's check, and I know that straw purchasers are often provided cash that is later converted to a cashier's check for the transaction.

31. Telephone toll records for Joe ROBLES's cellular phone indicate that ROBLES regularly exchanges phone calls and text messages with phone numbers with Las Vegas area codes. Based on my interview of Joe ROBLES, I also know that he was born and raised in Las Vegas, Nevada.

### **SUSPECT CONNECTIONS**

32. Agents located a Facebook profile for Joe ROBLES (URL: <https://www.facebook.com/bigojoe>, Facebook ID 219702491), by comparing ROBLES's

Wisconsin Department of Transportation photo with photos on the public page for Facebook profile "Joe Robles." The Wisconsin Department of Transportation photo for Joe Robles is consistent with the photos on the Facebook page for "Joe Robles."

33. Agents the searched the "friends" section of the Facebook page "Joe Robles" and found that ROBLES is "friends" with Facebook profiles "Rudy Robles" and "Roland Munoz." The Nevada Department of Transportation photo for Rudy Robles is consistent with the profile photo for Facebook profile "Rudy Robles" (URL: <https://www.facebook.com/rudy.robles.984>, Facebook ID 600962537). The Facebook profile "Rudy Robles" is also "friends" with the Facebook profile "Roland Munoz," "Joe Robles," and "Kaitlin Robles," Joe Robles's wife.

34. The Nevada Department of Transportation photo for Roland MUNOZ is consistent with the profile photo for Facebook profile "Roland Munoz" (URL: <https://www.facebook.com/roland.munoz.10>, Facebook ID 100007628077165). The Facebook profile "Roland Munoz" is also "friends" with the Facebook profiles "Rudy Robles" and "Joe Robles."

35. During a search of the public page for Facebook profile "Rudy Robles," agents found the following photo dated February 11, 2019 depicting Rudy ROBLES and Joe ROBLES:



### **INTERVIEWS OF JOE ROBLES AND KYLE MILLIGAN**

36. On the morning of September 6, 2019, I interviewed Joe ROBLES at a federal firearms licensee in Green Bay, Wisconsin, when ROBLES arrived to retrieve two DS Arms RPDs, 7.62x39 caliber, belt-fed rifles purchased on Gunbroker.com. During the interview, Joe ROBLES confirmed that he knew Rudy ROBLES and Roland MUNOZ. He also confirmed that he had purchased an additional DS Arms RPD rifle at a federal firearms licensee in Waukesha, Wisconsin. ROBLES advised that he had also purchased an M2 Browning, an M240, and a tripod for an M2 Browning. He stated that he also owned a shotgun and a 30/30 rifle.

37. Agents informed ROBLES that he purchased approximately \$31,000 worth of firearms since May 2019.<sup>1</sup>

---

<sup>1</sup> In total, Joe Robles has now purchased approximately \$35,000 in firearms after the purchase of an additional DS Arms RPD rifle.

38. ROBLES informed agents that he and his wife collectively made approximately \$110,000 per year. ROBLES' explained that their income was derived from his cellular phone repair business and his wife's dental hygienist position. Records from the Wisconsin Department of Workforce Development, however, revealed that the 2018 income for ROBLES and his wife was only \$62,297. He stated that he had received approximately \$15,000 for his wedding and approximately \$10,000 to \$12,000 per year for his business as a disc jockey.

39. ROBLES also explained that he had approximately \$12,000 in student loan debt.

40. ROBLES assured agents that he still possessed all of the firearms. Agents explained to ROBLES that the type of firearms purchases in comparison to his income is an indicator of firearms trafficking. Agents also explained they were aware of his connections to Rudy ROBLES and Roland MUNOZ in Las Vegas, Nevada, and ROBLES confirmed that he knew them and provided a telephone number with which he had communicated with Rudy ROBLES.

41. Agents asked to see and obtain photographs of the firearms. ROBLES produced his phone and showed agents photographs of a belt-fed rifle, similar to an M240, which his wife was reportedly holding. Agents informed ROBLES that they needed to physically inspect the firearms that day, and ROBLES indicated that they were not all at his house and that some might be at a cabin. ROBLES advised that he goes shooting with Kyle MILLIGAN and that he purchased the firearms to shoot with MILLIGAN. Agents advised ROBLES that they did not believe his explanation and asked if he wanted to be truthful. ROBLES responded that he needed

to “talk to my people.”

42. Agents performed a NCIC check of Joe ROBLES and found that he has no criminal history.

43. Later on September 6, 2019, ATF agents interviewed KYLE MILLIGAN in Green Bay, Wisconsin. During the interview, MILLIGAN informed agents that he ordered two rifles from Gunbroker.com, a DS Arms RPD 7.62 belt-fed rifle, bearing serial number WR0213, and a FNH USA, M249S Para, belt-fed rifle, bearing serial number M249SA07105. MILLIGAN stated that a Hispanic-American male that he knew as “Fernando” from El Paso, Texas, provided MILLIGAN the cash to purchase the rifles in a McDonald’s parking lot just north of Milwaukee.

44. MILLIGAN explained that Joe ROBLES organized the meeting. MILLIGAN later provided consent to search his phone with him present. Agents identified text messages from a contact saved as “Joe Robles” and believes this to be Joe ROBLES. Those text messages corroborated MILLIGAN’s statement, in that “Joe Robles” sent a text message to MILLIGAN on July 6, 2019 providing the address of 5344 North Port Washington Road in Glendale, Wisconsin. “Joe Robles” then sent a text message stating: “It’s a mc Donald’s.”

45. On July 7, 2019, ROBLES texted the contact information for an FFL in Green Bay. MILLIGAN advised that this is where ROBLES directed him to ship the rifles as a part of the Gunbroker.com transaction.

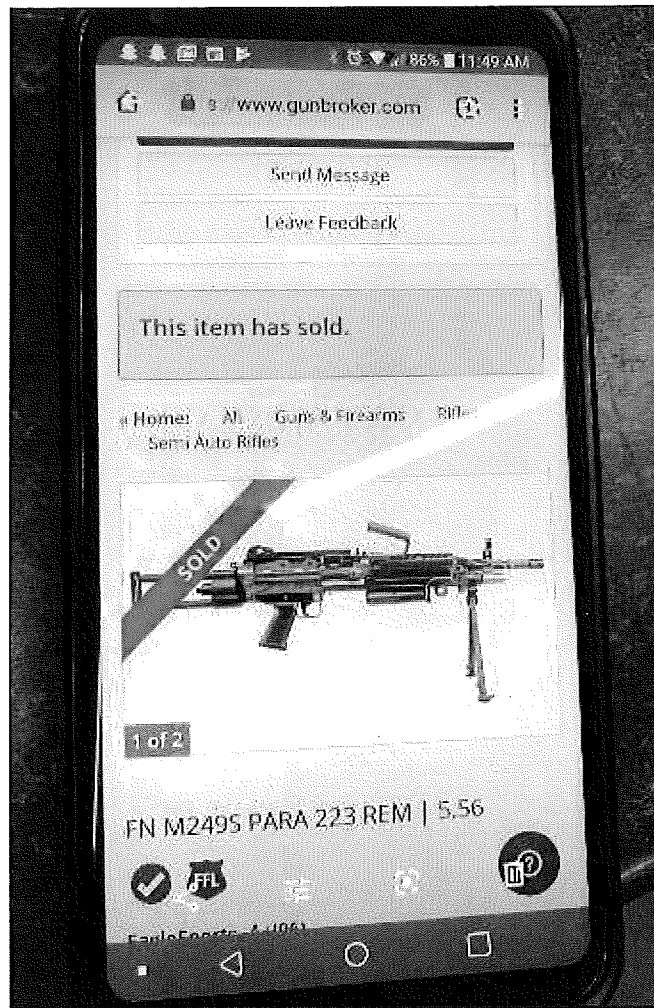
46. MILLIGAN indicated that he obtained the firearms from the FFL in Green Bay on July 21, 2019. MILLIGAN advised that he provided these firearms to “Fernando” in

exchange for a few hundred to one thousand dollars. MILLIGAN advised that he transferred these firearms to “Fernando” at Joe ROBLES’s cell phone repair store and vape shop on the west side of Green Bay. Agents know that MILLIGAN was referring to Joe ROBLES’s business iSupply West + Vape - Electronic Repairs and Sales, located at 1315 West Mason Street, Unit 1, Green Bay, Wisconsin 54303.

47. MILLIGAN advised that he also went to a bar with “Fernando.” While reviewing MILLIGAN’s cellular phone, agents observed the following text messages between MILLIGAN and Joe ROBLES on July 21, 2019—the date of the transfer:

- ROBLES: Our Mexican family wants to get drinks tonight
- MILLIGAN: Mexican family
- ROBLES: Fernando
- ROBLES: ?
- ROBLES: But not till nine
- MILLIGAN: So not going out?
- ROBLES: Yeah I’m out lol
- ROBLES: Go to latern be there in about 20

48. I reviewed photographs on MILLIGAN’s phone with him and observed a Gunbroker.com screenshot indicating that an FN M249S PARA belt-fed rifle had been sold. MILLIGAN confirmed that this was the firearm that he purchased for “Fernando.”



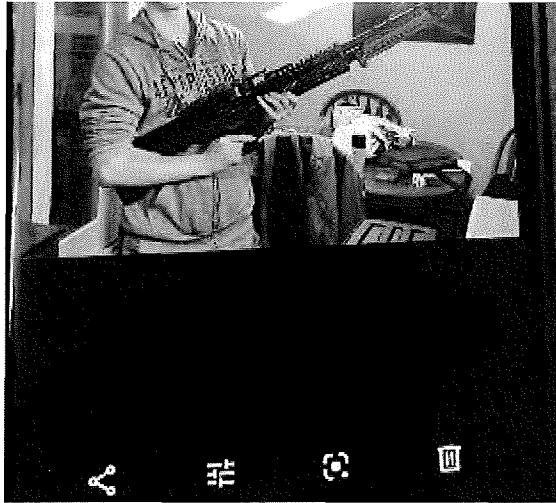
49. I also observed a photograph of MILLIGAN holding cash wrapped in rubber bands next to his head. MILLIGAN informed agents that this was the money Joe ROBLES received for the firearms that he purchased.





50. Next, I observed a photograph of MILLIGAN holding a belt-fed rifle.

MILLIGAN explained that this was ROBLES's firearm and that the photograph was taken at ROBLES' residence.



51. I also observed a photograph on MILLIGAN's phone depicting a box of linked ammunition used in belt-fed rifles. MILLIGAN informed agents that this ammunition belonged to ROBLES, but that he received a belt of the linked ammunition that he kept for himself.



52. MILLIGAN informed agents that “Fernando” stayed at the Hotel J on Packerland and drove a white van with a California license plate. MILLIGAN indicated that he may have been at the hotel on the date that MILLIGAN received the firearms from the FFL—July 21, 2019. In reviewing MILLIGAN’s phone, agents observed a text message dated July 21, 2019 from MILLIGAN to ROBLES that corroborated MILLIGAN’s statement. That text message stated in substance: “Getting in Packerland now.”

53. For several reasons, case agents believe that MILLIGAN is reliable and credible. MILLIGAN has no criminal record according to an NCIC check performed by agents. The information that he provided is substantially against his penal interests. MILLIGAN admitted to the straw purchase of multiple firearms for an individual who he believed was Mexican and lived in El Paso, Texas. MILLIGAN appears to have had an adequate opportunity to directly observe the events described above. The information provided by MILLIGAN is consistent with evidence obtained elsewhere in this investigation and is corroborated by text messages and photographs observed by agents on MILLIGAN's phone and independent investigation, including information from other sources, as described below. Finally, MILLIGAN advised agents that he would continue to assist agents in their investigation and consented to the search of his phone.

#### **IDENTIFICATION OF "FERNANDO"**

54. After completing the interviews, ATF agents drove to the Hotel J located at 2620 Packerland Drive in Green Bay, Wisconsin. Agents obtained check-in information indicating that "Fernando MOLINAR" of 348 Emerald Way, El Paso, Texas and with telephone number (949) 395-7532 stayed at Hotel J on July 21, 2019—the date of MILLIGAN's firearm purchase and meeting at the bar.

#### **IDENTIFICATION OF SEARCH LOCATIONS**

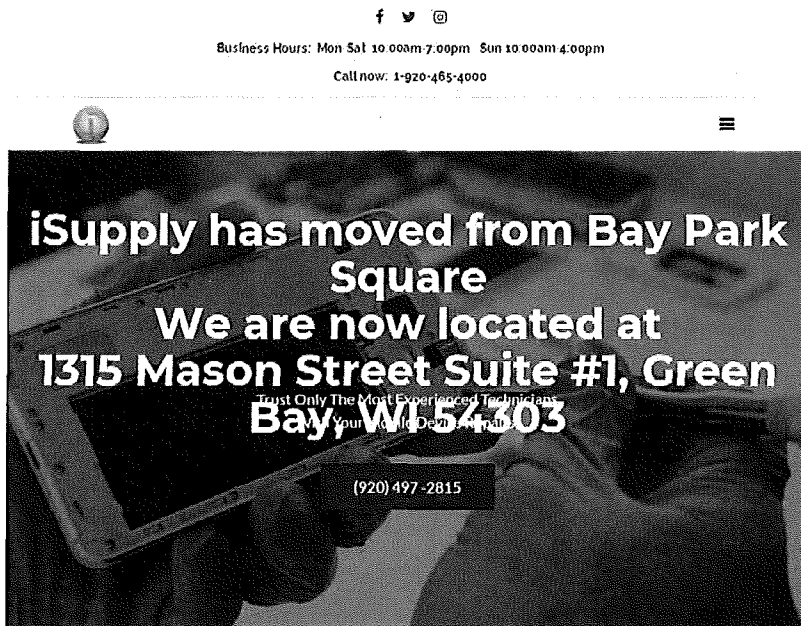
55. Agents believe that Joe ROBLES resides at 915 North Locust Street, Green Bay, Wisconsin 54303. This is the current address listed on Joe ROBLES's Wisconsin driver license.

Joe ROBLES also provided this address on his ATF Form 4473s during his firearms transfers on May 30, 2019 and June 21, 2019 and his attempted transfer on July 12, 2019. Finally, Joe ROBLES provided this as his home address during his interview with case agents on September 6, 2019.

56. Agents also believe that Joe ROBLES owns and operates iSupply West Vape - Electronic Repairs and Sales, located at 1315 West Mason Street, Unit 1, Green Bay, Wisconsin 54303. Joe ROBLES stated to agents that he owned iSupply cell phone repair shops. Agents observed deposits into Joe ROBLES bank account from iSupply. Additionally, MILLIGAN told agents that Joe ROBLES owned and operated iSupply vape and cell phone repair shops.

57. Agents are aware that there is an additional address for iSupply East + Vape - Electronic Repair and Sales Shop: 2245 Main Street, Unit 1, Green Bay, WI, 54302. However, the website for iSupply (<https://www.goisupply.com/>) indicates that iSupply recently moved to the location on West Mason Street, as depicted below:





58. Agents believe that MILLIGAN resides at 2100 Memorial Drive, Apartment 204, Green Bay, Wisconsin 54303. It is the listed address on MILLIGAN's Wisconsin driver license. MILLIGAN provided that address on ATF Form 4473 during the firearms transfers on July 21, 2019. MILLIGAN's roommate confirmed that he had lived with MILLIGAN at that address. Finally, MILLIGAN provided this as his home address during his interview with case agents on September 6, 2019.

59. As described above, there is probable cause to believe that evidence of these crimes is contained on Joe ROBLES's cellphone and that this cellphone is an instrumentality of these crimes. There is also probable cause to believe that Joe ROBLES's cellphone will be found on his person or in his presence. Based on my training and experience, I know that people often

carry their cellular devices on their person or in their presence. There is also probable cause to believe that evidence of firearms transactions (such as receipts), financial information (such as credit cards, debit cards, checks, and bank records), and the proceeds of the crimes described above will be found on his person or in his personal effects. I know that people often keep and carry receipts, credit cards, debit cards, checks, currency, and other financial information in wallets, purses, and other personal effects. For that reason, there is probable cause to search the person of Joe ROBLES and to seize the items described in Attachment B4.

#### **ELECTRONIC STORAGE AND FORENSIC ANALYSIS**

60. As described above and in Attachments B1, B2, B3, and B4, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrants applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

61. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- i. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via

the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- ii. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- iii. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.



- iv. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

62. *Forensic evidence.* As further described in Attachments B1, B2, B3, and B4, these applications seek permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrants, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

- i. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record

information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

- ii. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpatory or exculpatory the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and

durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or

consciousness of guilt (e.g., running a “wiping” program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- iii. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- iv. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrants.
- v. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the

presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

63. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrants. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- i. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrants call for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrants can take weeks or months,

depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

- ii. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- iii. Variety of forms of electronic media. Records sought under these warrants could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

64. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrants I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrants, and would authorize a later review of the media or information consistent with the warrants. The later review may require techniques, including but not limited to computer-assisted

scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrants.

65. Because several people share the PREMISES listed in Attachments A1, A2, and A3 as residences and a business, it is possible that the PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that it is possible that the things described in these warrants could be found on any of those computers or storage media, the warrants applied for would permit the seizure and review of those items as well.

#### **TECHNICAL TERMS**

66. I use the following technical terms to convey the following meanings:

67. IP Address: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

68. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices

communicating with each other are in the same state.

### **CONCLUSION**

69. I submit that this affidavit supports probable cause for warrants to search the property described in Attachments A1, A2, A3, and A4, and seize the items described in Attachments B1, B2, B3, and B4, respectively.

### **REQUEST FOR SEALING**

70. I further request that the Court order that all papers in support of these applications, including the affidavits and search warrants, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.



**ATTACHMENT A1**

**Property to be searched**

The property to be searched is the premises located at **915 North Locust Street, Green Bay, Wisconsin 54303**, more fully described as a single story, single family brick residence with a grey roof. That premises has an attached single garage painted white to the south of the front door and a chain link fence on the north side of the residence.



## ATTACHMENT A2

### **Property to be searched**

The property to be searched is the premises located at **2100 Memorial Drive, Apartment 204, Green Bay, Wisconsin 54303**, more fully described as a two-bedroom apartment located in the Northern Pines Apartment Complex. The apartment complex is a two story structure with cream and white colored siding and a grey roof. Unit 204 is located on the second story of the building with the numerals “204” prominently displayed on the front door to the apartment.







### ATTACHMENT A3

#### **Property to be searched**

The property to be searched is the premises of **iSupply West + Vape – Electronic Repairs and Sales**, more fully described as a business located at 1315 West Mason Street, Unit 1, Green Bay, Wisconsin 54303. This business is located in the Ridgeview Center, which contains approximately four separate businesses. The building is white and stone in color with black support beams and a brown roof. The numerals “1315” are prominently displayed on the sign directly in front of the building. The business bears a white sign with the words “i supply vape” located directly above the front door entrance.



**ATTACHMENT A4**

**Property to be searched**

The property to be searched is the person of Joe Robles (DOB: 11/10/1986).

## **ATTACHMENT B1**

### *Property to be seized*

1. ATF Form 4473s, firearms, firearm boxes, bipods, tripods, upper receivers, receipts and any records related to firearms, firearms accessories, ammunition, financial documents that transfer of proceeds of the above schemes, computers, electronics capable of communication, and cellphones such as:

- a. lists of contacts and any identifying information;
- b. photographs, videos, or other media storage connected to firearms;
- c. types, amounts, and prices of firearms purchased/sold;
- d. any information related to sources or purchasers of firearms (including names, addresses, phone numbers, or any other identifying information);
- e. all bank records, checks, credit card bills, account information, and other financial records related to firearms commerce;
- f. any and all financial records connected to the purchase/sale of firearms;

2. Cellphones, computers, and all media storage devices that may hold documentation regarding firearm or ammunition purchases/sales and customers;

3. Any and all financial records connected to the purchase/sale of firearms, and any correspondence between suspects and other firearms sellers and/or purchasers;

4. All bank records, checks, credit card bills, account information, and other financial records related to firearms commerce;

5. Proceeds of firearms trafficking activities, including United States currency;



6. All bank records, checks, credit card bills, account information, and other financial records; Financial records, documents, statements, or other evidence of control of bank or other financial accounts and investment funds;

7. Personal address books, telephone bills, photographs, letters, personal notes, documents and other items or lists reflecting names, addresses, telephone numbers, addresses and communications regarding illegal activities among and between members and associates involved in firearms trafficking activities;

8. Documents and deeds reflecting the purchase or lease of items obtained with the proceeds from firearm trafficking activities;

9. Records of off-site locations to store proceeds and other records, including safes, vaults, or lock boxes, safe deposit box keys, records and receipts and rental agreements for storage facilities;

10. Records of mail and communications services, cellular telephones and all electronic storage areas on the device including stored telephone numbers, recently called numbers list, text messages, digital audio and or video recordings, pictures, settings, and any other user defined settings and/or data;

11. Indicia of occupancy, residency or ownership of the premises, including utility bills, telephone bills, loan payment receipts, addressed envelopes, escrow documents and keys;

12. Evidence of user attribution showing who used or owned the devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

13. As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

14. All records relating to violations of 18 U.S.C. § 922(a)(1)(A) (engaging in a firearms business without a license), 18 U.S.C. § 922(d) (transferring a firearm to a prohibited person), 18 U.S.C. § 922(a)(6) (false statement to a federal firearms licensee), 18 U.S.C. § 924(b) (interstate or foreign transport of a firearm for a felony purpose), 18 U.S.C. § 922(a)(9) (unlawful receipt of firearms), 18 U.S.C. § 924(h) (transfer of firearm to be used in drug trafficking crime or crime of violence), 18 U.S.C. § 924(g) (interstate travel and transfer with intent to commit drug trafficking crime or crime of violence), 22 U.S.C. § 2778(b)(2)(c) (illegal export of munitions), and 18 U.S.C. § 371 (conspiracy), involving suspects and conspirators, known or unknown, occurring after April 15, 2017, including:

- a. Records and information relating to a conspiracy traffic firearms;
- b. Records and information relating to the e-mail and Facebook accounts names in the affidavit;
- c. Records and information relating to the identity or location of the suspects;
- d. Records and information relating to communications with Internet Protocol addresses;
- e. Records and information relating to the crimes referenced in Attachment B, paragraph 14.



15. Computers or storage media used as a means to commit the violations described above;

16. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
- b. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- c. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
- d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- f. evidence of the times the COMPUTER was used;
- g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

- h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- i. records of or information about Internet Protocol addresses used by the COMPUTER;
- j. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- k. contextual information necessary to understand the evidence described in this attachment.

17. As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

18. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

19. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

## ATTACHMENT B2

### *Property to be seized*

1. ATF Form 4473s, firearms, firearm boxes, bipods, tripods, upper receivers, receipts and any records related to firearms, firearms accessories, ammunition, financial documents that transfer of proceeds of the above schemes, computers, electronics capable of communication, and cellphones such as:

- a. lists of contacts and any identifying information;
- b. photographs, videos, or other media storage connected to firearms;
- c. types, amounts, and prices of firearms purchased/sold;
- d. any information related to sources or purchasers of firearms (including names, addresses, phone numbers, or any other identifying information);
- e. all bank records, checks, credit card bills, account information, and other financial records related to firearms commerce;
- f. any and all financial records connected to the purchase/sale of firearms;

2. Cellphones, computers, and all media storage devices that may hold documentation regarding firearm or ammunition purchases/sales and customers;

3. Any and all financial records connected to the purchase/sale of firearms, and any correspondence between suspects and other firearms sellers and/or purchasers;

4. All bank records, checks, credit card bills, account information, and other financial records related to firearms commerce;

5. Proceeds of firearms trafficking activities, including United States currency;

6. All bank records, checks, credit card bills, account information, and other financial records; Financial records, documents, statements, or other evidence of control of bank or other financial accounts and investment funds;

7. Personal address books, telephone bills, photographs, letters, personal notes, documents and other items or lists reflecting names, addresses, telephone numbers, addresses and communications regarding illegal activities among and between members and associates involved in firearms trafficking activities;

8. Documents and deeds reflecting the purchase or lease of items obtained with the proceeds from firearm trafficking activities;

9. Records of off-site locations to store proceeds and other records, including safes, vaults, or lock boxes, safe deposit box keys, records and receipts and rental agreements for storage facilities;

10. Records of mail and communications services, cellular telephones and all electronic storage areas on the device including stored telephone numbers, recently called numbers list, text messages, digital audio and or video recordings, pictures, settings, and any other user defined settings and/or data;

11. Indicia of occupancy, residency or ownership of the premises, including utility bills, telephone bills, loan payment receipts, addressed envelopes, escrow documents and keys;

12. Evidence of user attribution showing who used or owned the devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

13. As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

14. All records relating to violations of 18 U.S.C. § 922(a)(1)(A) (engaging in a firearms business without a license), 18 U.S.C. § 922(d) (transferring a firearm to a prohibited person), 18 U.S.C. § 922(a)(6) (false statement to a federal firearms licensee), 18 U.S.C. § 924(b) (interstate or foreign transport of a firearm for a felony purpose), 18 U.S.C. § 922(a)(9) (unlawful receipt of firearms), 18 U.S.C. § 924(h) (transfer of firearm to be used in drug trafficking crime or crime of violence), 18 U.S.C. § 924(g) (interstate travel and transfer with intent to commit drug trafficking crime or crime of violence), 22 U.S.C. § 2778(b)(2)(c) (illegal export of munitions), and 18 U.S.C. § 371 (conspiracy), involving suspects and conspirators, known or unknown, occurring after April 15, 2017, including:

- a. Records and information relating to a conspiracy traffic firearms;
- b. Records and information relating to the e-mail and Facebook accounts names in the affidavit;
- c. Records and information relating to the identity or location of the suspects;
- d. Records and information relating to communications with Internet Protocol addresses;
- e. Records and information relating to the crimes referenced in Attachment B, paragraph 14.

15. Computers or storage media used as a means to commit the violations described above;

16. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
- b. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- c. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
- d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- f. evidence of the times the COMPUTER was used;
- g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

- h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- i. records of or information about Internet Protocol addresses used by the COMPUTER;
- j. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- k. contextual information necessary to understand the evidence described in this attachment.

17. As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

18. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

19. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

### **ATTACHMENT B3**

#### *Property to be seized*

1. ATF Form 4473s, firearms, firearm boxes, bipods, tripods, upper receivers, receipts and any records related to firearms, firearms accessories, ammunition, financial documents that transfer of proceeds of the above schemes, computers, electronics capable of communication, and cellphones such as:

- a. lists of contacts and any identifying information;
- b. photographs, videos, or other media storage connected to firearms;
- c. types, amounts, and prices of firearms purchased/sold;
- d. any information related to sources or purchasers of firearms (including names, addresses, phone numbers, or any other identifying information);
- e. all bank records, checks, credit card bills, account information, and other financial records related to firearms commerce;
- f. any and all financial records connected to the purchase/sale of firearms;

2. Cellphones, computers, and all media storage devices that may hold documentation regarding firearm or ammunition purchases/sales and customers;

3. Any and all financial records connected to the purchase/sale of firearms, and any correspondence between suspects and other firearms sellers and/or purchasers;

4. All bank records, checks, credit card bills, account information, and other financial records related to firearms commerce;

5. Proceeds of firearms trafficking activities, including United States currency;



6. All bank records, checks, credit card bills, account information, and other financial records; Financial records, documents, statements, or other evidence of control of bank or other financial accounts and investment funds;

7. Personal address books, telephone bills, photographs, letters, personal notes, documents and other items or lists reflecting names, addresses, telephone numbers, addresses and communications regarding illegal activities among and between members and associates involved in firearms trafficking activities;

8. Documents and deeds reflecting the purchase or lease of items obtained with the proceeds from firearm trafficking activities;

9. Records of off-site locations to store proceeds and other records, including safes, vaults, or lock boxes, safe deposit box keys, records and receipts and rental agreements for storage facilities;

10. Records of mail and communications services, cellular telephones and all electronic storage areas on the device including stored telephone numbers, recently called numbers list, text messages, digital audio and or video recordings, pictures, settings, and any other user defined settings and/or data;

11. Indicia of occupancy, residency or ownership of the premises, including utility bills, telephone bills, loan payment receipts, addressed envelopes, escrow documents and keys;

12. Evidence of user attribution showing who used or owned the devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

13. As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

14. All records relating to violations of 18 U.S.C. § 922(a)(1)(A) (engaging in a firearms business without a license), 18 U.S.C. § 922(d) (transferring a firearm to a prohibited person), 18 U.S.C. § 922(a)(6) (false statement to a federal firearms licensee), 18 U.S.C. § 924(b) (interstate or foreign transport of a firearm for a felony purpose), 18 U.S.C. § 922(a)(9) (unlawful receipt of firearms), 18 U.S.C. § 924(h) (transfer of firearm to be used in drug trafficking crime or crime of violence), 18 U.S.C. § 924(g) (interstate travel and transfer with intent to commit drug trafficking crime or crime of violence), 22 U.S.C. § 2778(b)(2)(c) (illegal export of munitions), and 18 U.S.C. § 371 (conspiracy), involving suspects and conspirators, known or unknown, occurring after April 15, 2017, including;

- a. Records and information relating to a conspiracy traffic firearms;
- b. Records and information relating to the e-mail and Facebook accounts names in the affidavit;
- c. Records and information relating to the identity or location of the suspects;
- d. Records and information relating to communications with Internet Protocol addresses;
- e. Records and information relating to the crimes referenced in Attachment B, paragraph 14.

15. Computers or storage media used as a means to commit the violations described above;

16. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
- b. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- c. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
- d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- f. evidence of the times the COMPUTER was used;
- g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

- h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- i. records of or information about Internet Protocol addresses used by the COMPUTER;
- j. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- k. contextual information necessary to understand the evidence described in this attachment.

17. As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

18. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

19. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

## **ATTACHMENT B4**

### *Property to be seized*

1. ATF Form 4473s, firearms, firearm boxes, bipods, tripods, upper receivers, receipts and any records related to firearms, firearms accessories, ammunition, financial documents that transfer of proceeds of the above schemes, computers, electronics capable of communication, and cellphones such as:

- a. lists of contacts and any identifying information;
- b. photographs, videos, or other media storage connected to firearms;
- c. types, amounts, and prices of firearms purchased/sold;
- d. any information related to sources or purchasers of firearms (including names, addresses, phone numbers, or any other identifying information);
- e. all bank records, checks, credit card bills, account information, and other financial records related to firearms commerce;
- f. any and all financial records connected to the purchase/sale of firearms;

2. Cellphones, computers, and all media storage devices that may hold documentation regarding firearm or ammunition purchases/sales and customers;

3. Any and all financial records connected to the purchase/sale of firearms, and any correspondence between suspects and other firearms sellers and/or purchasers;

4. All bank records, checks, credit card bills, account information, and other financial records related to firearms commerce;

5. Proceeds of firearms trafficking activities, including United States currency;

6. All bank records, checks, credit card bills, account information, and other financial records; Financial records, documents, statements, or other evidence of control of bank or other financial accounts and investment funds;

7. Personal address books, telephone bills, photographs, letters, personal notes, documents and other items or lists reflecting names, addresses, telephone numbers, addresses and communications regarding illegal activities among and between members and associates involved in firearms trafficking activities;

8. Documents and deeds reflecting the purchase or lease of items obtained with the proceeds from firearm trafficking activities;

9. Records of off-site locations to store proceeds and other records, including safes, vaults, or lock boxes, safe deposit box keys, records and receipts and rental agreements for storage facilities;

10. Records of mail and communications services, cellular telephones and all electronic storage areas on the device including stored telephone numbers, recently called numbers list, text messages, digital audio and or video recordings, pictures, settings, and any other user defined settings and/or data;

11. Indicia of occupancy, residency or ownership of the premises, including utility bills, telephone bills, loan payment receipts, addressed envelopes, escrow documents and keys;

12. Evidence of user attribution showing who used or owned the devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

13. As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

14. All records relating to violations of 18 U.S.C. § 922(a)(1)(A) (engaging in a firearms business without a license), 18 U.S.C. § 922(d) (transferring a firearm to a prohibited person), 18 U.S.C. § 922(a)(6) (false statement to a federal firearms licensee), 18 U.S.C. § 924(b) (interstate or foreign transport of a firearm for a felony purpose), 18 U.S.C. § 922(a)(9) (unlawful receipt of firearms), 18 U.S.C. § 924(h) (transfer of firearm to be used in drug trafficking crime or crime of violence), 18 U.S.C. § 924(g) (interstate travel and transfer with intent to commit drug trafficking crime or crime of violence), 22 U.S.C. § 2778(b)(2)(c) (illegal export of munitions), and 18 U.S.C. § 371 (conspiracy), involving suspects and conspirators, known or unknown, occurring after April 15, 2017, including:

- a. Records and information relating to a conspiracy traffic firearms;
- b. Records and information relating to the e-mail and Facebook accounts names in the affidavit;
- c. Records and information relating to the identity or location of the suspects;
- d. Records and information relating to communications with Internet Protocol addresses;
- e. Records and information relating to the crimes referenced in Attachment B, paragraph 14.

15. Computers or storage media used as a means to commit the violations described above;

16. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
- b. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- c. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
- d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- f. evidence of the times the COMPUTER was used;
- g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;



- h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- i. records of or information about Internet Protocol addresses used by the COMPUTER;
- j. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- k. contextual information necessary to understand the evidence described in this attachment.

17. As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

18. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

19. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.